Published on *The National Law Review* https://natlawreview.com

CCPA Business-to-Business and Employment Information Exceptions Ending

Article By:

Steven M. Millendorf

Eileen R. Ridley

Leighton B. R. Allen

As the California Privacy Rights Act (CPRA) comes into effect on January 1, 2023, the temporary and partial exceptions for employment and business-to-business information will expire, making California the first and only state with a general privacy law that applies to this type of information. The current partial exceptions, which were proposed in 2019 as part of a set of amendments to the California Consumer Privacy Act (CCPA), were originally extended again until January 1, 2023 as part of the ballot initiative that enacted the CPRA. While multiple bills were proposed to extend the partial exceptions either by one additional year or indefinitely, all of the proposed bills failed to make it out of committee and passed by the California legislature by August 31, 2022, the last day for such bills to be passed in the legislative year.

What Is Employment-Related Information and Business-to-Business Information?

The current exceptions included many, but not all, of the provisions in the CCPA relating to employment and business to business information. The employment information exception applied to personal information collected by a business about a consumer acting as a job applicant or who is a past or current employee of, owner of, director of, officer of, medical staff member of, or contractor of the business and their beneficiaries and dependents (**Employment-Related Information**), so long as the business used the information solely in the context of the employment relationship. Under the CCPA's exception for Employment-Related Information, the business was only required to provide the employee with a shortened privacy notice and the CCPA provided the employee with a private right of action in the event of a data breach where the business failed to use reasonable security measures. Businesses should be reminded that "personal information" under the CPRA is defined broadly, and Employment-Related Information may now include things like network monitoring, video surveillance, photographs, and document metadata. It may also biometric data (including fingerprints and face and voice recognition when used to identify or authenticate the employee), which may be

applicable to some businesses. Businesses should also be aware that biometric data may come under other stringent privacy statutes in and of itself (e.g., *see,* the Biometric Information Privacy Act in Illinois – 740 ILCS 14 and California SB 1189).

The business-to-business exception applied to personal information collected and used by the business about a consumer acting as an employee, owner, director, officer, or contractor of another company, partnership, sole proprietorship, nonprofit, or government entity, but solely to the extent the business used this personal information in the context of conducting due diligence regarding, or providing or receiving a product or service to such company, partnership, sole proprietorship, nonprofit, or government agency (**B2B Information**). Under the CCPA, businesses were only required to provide the consumer with an opportunity to opt-out of the disclosure of their B2B Information for monetary or other valuable consideration (i.e., a "sale" under the CCPA), if any, but was not required to provide a privacy notice and the CCPA did not otherwise provide a private right of action for data breaches.

Which Requirements Under the CPRA will apply to Employment-Related Information and Business-to-Business Information?

With the partial exceptions for Employment-Related Information and B2B Information expiring, the CPRA in its entirety will apply to these categories. This includes:

- Requirements to provide consumers with privacy notices that meet all of the privacy notice requirements of the CPRA and address the collection and use of Employment-Related Information and B2B Information.

- Consumer rights, such as the right to know (access), right to deletion, and the right to correction. The CPRA also eliminates the one-year lookback period such that businesses may need to produce Employment-Related Information and B2B Information that goes as far back as its data retention period for these. This brings the CPRA more in line with the requirements of the GDPR.

- Right to opt-out of the sale (as defined in the CPRA) of the Employment-Related Information and B2B Information or the disclosure of such information for cross-context behavioral advertising.

- Right to limit the use of sensitive personal information for purposes other than the specific purposes enumerated in the CPRA regulations.

- Contractual obligations with service providers, contractors, and other third parties. With Employment-Related Information and B2B Information, this would include things like payroll providers, benefits providers, CRM systems, etc.

While current and former employees, job applicants, and business relations should always have been counted for the purposes of determining whether a business met the thresholds for CCPA, the full applicability of the CPRA to Employment-Related Information and B2B Information underscores the need to consider these individuals for the purpose of determining the applicability of the CPRA.

Impact on Businesses and the Use of Data

Businesses that are subject to both the CPRA and the GDPR should be familiar with the application of privacy requirements and data subject rights to Employment-Related Information and B2B Information, as the GDPR made no distinction between these classes of individuals and other data subjects. However, the expiration of the partial exceptions increase the compliance burden for businesses that are subject to the CPRA but not the GDPR. Such businesses should:

- Update privacy notices for Employment-Related Information and B2B Information. Businesses should consider separating out such privacy notices from their privacy notices to general consumers when appropriate.

- Amend agreements with service providers who may be involved in handling Employment-Related Information and B2B Information to comply with the contractual requirements for service providers and contractors under the CPRA. For Employment-Related Information, such service providers may include benefits providers, payroll providers, building managers, and other similar organizations who may have access to Employment-Related Information. For B2B Information, businesses should consider amending agreements with vendors who provide CRM services, postal and email services, and other similar organizations.

- Update data maps to include Employment-Related Information and B2B Information if not previously covered by data mapping exercises.

- Update internal policies and procedures for processing requests from consumers to exercise their access, deletion, and correction rights.

Impact on Employment-Related Information

The right of a consumer to access, delete, and correct their personal information may be especially troubling for Employment-Related Information. Employment-Related Information may include information that the business needs to keep confidential, such as the raw feedback related to performance appraisals, information about investigation activities, hiring/firing/disciplinary decisions, and other similar information. Businesses should consider the applicability of the exemptions set forth in Section 1798.145 of the CPRA when developing policies and procedures to comply with consumer requests from current, past, and prospective employees, owners, directors, officers, medical staff members, and contractors (and their beneficiaries and dependents). Applicable exceptions may include:

- The business's ability to exercise or defend legal claims. This may permit a business to withhold disclosing certain information about ongoing investigations, although it likely will not permit a business to withhold information regarding a previous investigation that is closed.

- The rights provided to consumers under the CPRA does not adversely affect the rights and freedoms of other natural persons. This may permit a business to withhold some information about performance reviews provided by third parties if it would infringe on that third party's privacy or confidentiality rights.

- Medical information subject to HIPAA or California's Confidentiality of Medical Information Act is generally excluded from the scope of the CPRA. This may permit a business to not disclose information related to information they may have collected as part of providing employee healthcare benefits.

- Information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living is also generally excluded from the scope of CPRA. This type of information may be collected as part of background checks for employees and job applicants.

- In limited circumstances, businesses may be able to deny a consumer's request on the grounds that complying with the request would be impossible or involve disproportionate effort. The CPRA regulations define "disproportionate effort" to occur when the time and/or resources expended by the business to respond to the individual request significantly outweighs the benefit provided to the consumer by responding to the request, for example, when the data is not in a searchable or readily accessible format. This could occur with paper records stored in offsite archives or a video feed of employees entering the business's premises. However, businesses should be reminded that the CPRA regulations make it clear that a failure to put adequate processes and procedures in place to comply with consumer requests cannot claim "disproportionate effort" to deny a consumer request.

- A business may also be able to deny a consumer's request if it is "manifestly unfounded or excessive." This exception typically deals with data to complete transactions, detect security incidents, and to comply with the law. However, the proof burden in meeting this exception falls on the business and any reliance should be documented by the business.

Businesses should also carefully review their policies and procedures for redacting certain personal information from responses to access requests. Businesses may collect and use categories of personal information as part of Employment-Related Information that it doesn't collect from the rest of its consumers and which the CPRA regulations prevent the business from producing as part of a consumer access request. This includes a consumer's social security number, driver's license number or other government-issued identification number, financial account number, any health insurance or other medical identification number, account passwords, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. The CPRA regulations prohibit disclosure of the specific pieces of these types of personal information in response to a consumer access request, but must still disclose a generic description of this type of information when collected by the business.

Impact on B2B Information

The impact on B2B Information may be less troublesome than Employment-Related Information. Most businesses will not have as much sensitive information about their business relations, if any. Nevertheless, businesses should still consider if the exceptions described above apply to any B2B Information in light of a request from a consumer in the business-to-business context.

National Law Review, Volume XII, Number 249